
保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

# Akira 勒索軟體～鎖定大戶

2023 年 5 月 8 日發布

**點擊此處可獲取--最完整的賽門鐵克解決方案資訊**

我們賽門鐵克的監控系統最近公開通報一種自稱為『Akira』（攻擊者自己命名）的新勒索軟體變種。然而，它並不完全是原創，看起來是由 Conti 勒索軟體的原始碼來進行修改。

當一台電腦被成功入侵時，資料會被上傳到攻擊者的伺服器，在檔案被加密並附加 .akira 副檔名之前作為威脅受害者之用。隨後是相當冗長的勒索說明，指示受害者安裝 TOR 瀏覽器，以便瀏覽 Akira 聊天室，讓他們可以開始與攻擊者進行談判。

Akira 背後的組織還維護著一個洩密網站，他們在該網站上大辣辣公布某些遭其入侵的金融、建築和房地產等多個受害企業的名稱。


據報導，攻擊者向受害者索價數十萬至數百萬美元不等，這大概取決於該組織認為受害者的支付能力。

賽門鐵克已經於第一時間提供多種有效保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec **零時差**防護技術偵測到的惡意程式名稱及有效對應的防護機制：

**基於行為偵測技術(SONAR)的防護：**

- SONAR.Ransomware!g*
- SONAR.Ransom!gen98
- SONAR.Ransomconti!g1

**基於機器學習的防禦技術：**

- Heur.AdvML.C

**基於安全強化政策(適用於使用DCS)：**

Symantec Data Center Security (DCS) 預設的強化政策可提供針對 Akira 勒索軟體的零時差保護。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

*這表示存在多個名稱相似的檢測，例如：SONAR.Ransomware!g1、SONAR.Ransomware!g2 等。

欲深入瞭解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。
欲瞭解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。
欲瞭解有關賽門鐵克 (DCS：Data Center Security～資料中心安全的更多訊息，請點擊此處。

## 關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片）軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。( 美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員 )。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

## 關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。